10/522067
DT01 Rec'd PCT/PTC 21 JAN 2005

In the Claims

1. (Original) A method of providing secure transmissions from a smartcard reader, said method comprising the steps of:

encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information;

transmitting said encrypted signal to a remote location relative to said smartcard reader;

translating at said remote location said transmitted signal to another format useable by an access controller; and

controlling an access mechanism using said access controller dependent upon said translated signal.

2. (Original) The method according to claim 1, wherein said smartcard contains biometric data and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly.

3. (Original) The method according to claim 2, wherein said biometric data comprises fingerprint data.

4. (Currently amended) The method according to claim 2 ~~or 3,~~ wherein said biometric data is not transmitted to said remote location from said smartcard reader.

5. (Currently amended) The method according to claim 1, further comprising the step of providing access using said access mechanism if said translated signal is determined by said access controller to ~~authorise~~ authorize access.

6. (Original) The method according to claim 5, wherein said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation.

7. (Currently amended) The method according to ~~any one of claims 1-5,~~ claim 1 wherein said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code.

8. (Currently amended) The method according to ~~any one of claims 1-7,~~ claim 1 wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

9. (Original) The method according to claim 1, further comprising the step of encrypting communications between said smartcard and said smartcard reader.

10. (Currently amended) The method according to ~~any one of claims 1-9,~~ claim 1 wherein said encrypted signal is transmitted from said smartcard reader to a high security module at said remote location.

11. (Original) The method according to claim 10, wherein said high security module translates said encrypted signal to said other format.

12. (Currently amended) The method according to claim 10, wherein said smartcard reader and said high security module are separated by a distance of up to 1.2 ~~kilometres~~ kilometers.

13. (Currently amended) The method according to claim 10, wherein said smartcard reader and said high security module are separated by a distance of up to 15 ~~metres~~ meters.

14. (Currently amended) The method according to ~~any one of claims 1-13,~~ claim 1 wherein said translated signal is in a controller-specified format.

15. (Original) The method according to claim 14, wherein said controller-specified format is Wiegand format, or clock and data.

16. (Original) A system for providing secure transmissions from a smartcard reader, said system comprising:

a smartcard reader for encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information, and for transmitting said encrypted signal to a remote location relative to said smartcard reader;

a high security module for receiving said transmitted signal and translating said transmitted signal to another format useable by an access controller; and

an access controller for controlling an access mechanism using said access controller dependent upon said translated signal.

17. (Original) The system according to claim 16, wherein said smartcard contains biometric data, and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly

18. (Original) The system according to claim 17, wherein said biometric data comprise fingerprint data.

19. (Currently amended) The system according to claim 17 ~~or 18,~~ wherein said biometric data is not transmitted to said high security module from said smartcard reader.

20. (Currently amended) The system according to claim 16, further

comprising an access mechanism providing access if said translated signal is determined by said access controller to ~~authorise~~ authorize access.

21. (Original) The system according to claim 20, wherein said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation.

22. (Currently amended) The system according to ~~any one of claims 16-21,~~ claim 16 wherein said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code.

23. (Currently amended) The system according to ~~any one of claims 16-22,~~ claim 16 wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

24. (Original) The system according to claim 16, wherein communications between said smartcard and said smartcard reader are encrypted.

25. (Currently amended) The system according to claim 24, wherein said smartcard reader and said high security module are separated by a distance of up to 1.2 ~~kilometres~~ kilometers.

26. (Currently amended) The system according to claim 24, wherein said smartcard reader and said high security module are separated by a distance of up to 15 ~~metres~~ meters.

27. (Currently amended) The system according to ~~any one of claims 16-26,~~ claim 16 wherein said translated signal is in a controller-specified format.

28. (Original) The system according to claim 27, wherein said controller-specified format is Wiegand format, or clock and data.

29. (Original) An apparatus for providing secure transmissions from a smartcard reader, said apparatus comprising:

a smartcard reader for encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information;

means for transmitting said encrypted signal to a remote location relative to said smartcard reader;

means for translating at said remote location said transmitted signal to another format useable by an access controller; and

an access controller for controlling an access mechanism dependent upon said translated signal.

30. (Original) The apparatus according to claim 29, wherein said smartcard contains biometric data and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly.

31. (Original) The apparatus according to claim 30, wherein said biometric data comprises fingerprint data.